



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/847,813	05/01/2001	Curt Wohlgemuth	OMNI0008	6351

7590 02/16/2006  
PERKINS COIE LLP  
ATTN: Mr. Brian R. Coleman  
101 Jefferson Drive  
Menlo Park, CA 94025

EXAMINER

LANIER, BENJAMIN E

ART UNIT PAPER NUMBER

2132

DATE MAILED: 02/16/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b> 09/847,813	<b>Applicant(s)</b> WOHLGEMUTH ET AL.	
	<b>Examiner</b> Benjamin E Lanier	<b>Art Unit</b> 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 19 December 2005.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-3, 10-12, 19, 25 and 31-44 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-3, 10-12, 19, 25 and 31-44 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

## **DETAILED ACTION**

### ***Response to Amendment***

1. Applicant's amendment filed 19 December 2005 amends claims 1, 3, 10, 12, 19, 25, and 31-44. Applicant's amendment has been fully considered and is entered.

### ***Response to Arguments***

2. Applicant's arguments filed 19 December 2005 have been fully considered but they are not persuasive. Applicant's argument that claims 31-44 are allowable for the similar reasons that claim 1 is distinguished from Safadi is not persuasive because claims 31-44 do not require the network file system that was used to distinguish claim 1 over the Safadi reference. Therefore the rejections of claims 31-44 in view of Safadi will be maintained while the rejections of claims 1-3, 10-12, 19, and 25 in view of Safadi will be withdrawn.
3. Applicant's arguments, filed 19 December 2005, with respect to the amended claim language in view of England have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Vahalia, U.S. Patent No. 6,192,408.

### ***Claim Rejections - 35 USC § 102***

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Art Unit: 2132

5. Claims 1-3, 10-12, 19, 25, 31-44 are rejected under 35 U.S.C. 102(e) as being anticipated by Vahalia, U.S. Patent No. 6,192,408. Referring to claims 1, 10, Vahalia discloses a data storage system wherein a network file server containing an array of data movers, and a disk storage subsystem (Figure 1), provides high-end file server applications such as the Network File System (NFS) protocol standard (Col. 5, lines 40-43). The system processes and receives NFS data requests from a client computer (Col. 13, lines 66-67), which meets the limitation of providing a network file system on a client, wherein said network file system handles and forwards requests from streaming-enabled local processes on said client that are directed at streaming application programs files located on said server. The data is provided over the system in a streaming fashion (Col. 7, lines 13-29), which meets the limitation of targeted streaming application program files being requested and located on a server. The client terminal provides NFS data requests over the network that are processed by a data mover of the network file server (Col. 13, lines 66-67), which makes the limitation of streaming-enabled local processes on the client and inherent feature of Vahalia because the use of the NFS protocol requires streaming-enabled local processes. The data mover receiving the NFS request decodes the request to verify the RPC portion of the request and check's the client's authorization for the desired access (Col. 14, lines 1-5). If the request is not authenticated and authorized then execution of the request is rejected (Col. 14, lines 5-7). Otherwise, the request is granted (Col. 14, lines 7-8), which meets the limitation of wherein said network file system examines said requests, and either grants or denies each of said requests depending on whether the request is justifiable from a security perspective by using information that includes, but is not limited to: the nature of the originating streaming-enabled process, the history of previous access by the streaming-enabled process,

Art Unit: 2132

and/or the section of the targeted streaming application program file being requested. If the request is granted then the data mover processing the request discovers the path to the desired file and sends a request to the remote file system corresponding to the file for access (Col. 14, lines 9-35), which meets the limitation of providing a network redirector component of said network file system, and said network redirector component makes visible to said network file system, a path that represents the server where said streaming application program files are stored.

Referring to claims 2, 3, 11, 12, Vahalia discloses that a plurality of data movers are used to provide access to the read/write file systems (Col. 13, lines 29-31). Each read/write file system is assigned a primary data mover with respect to the file system (Col. 13, lines 31-33). This data mover has the exclusive right to directly access data in each file in the read/write file system, and manages the read and write locks on the files in the file system (Col. 13, lines 33-38). When a data mover receives a request for access from a client terminal, the data mover checks the type of request and the database of the file system for which it is serving to determine whether they can process the request or whether the request must be processed by a different data mover (Col. 13, lines 38-64), which meets the limitation of said network file system registers dispatch routines with the client operating system that handles common file operations such as open, read, write, and close, wherein a dispatch routine examines a file request and decides whether to grant or deny said file request, wherein if said file request is granted then said dispatch routine forwards said file request to said server and sends back said server's response to said client operating system, wherein when a local stream-enabled process on said client makes a file request for a

streaming application program file on said server, said client operating system calls a dispatch routine with said file request.

Referring to claims 19, 25, Vahalia discloses a data storage system wherein a network file server containing an array of data movers, and a disk storage subsystem (Figure 1), provides high-end file server applications such as the Network File System (NFS) protocol standard (Col. 5, lines 40-43). The system processes and receives NFS data requests from a client computer (Col. 13, lines 66-67), which meets the limitation of providing a network file system on a client, wherein said network file system handles and forwards requests from streaming-enabled local processes on said client. The data is provided over the system in a streaming fashion (Col. 7, lines 13-29), which meets the limitation of targeted streaming application program files being requested and located on a server. The client terminal provides NFS data requests over the network that are processed by a data mover of the network file server (Col. 13, lines 66-67), which makes the limitation of streaming-enabled local processes on the client and inherent feature of Vahalia because the use of the NFS protocol requires streaming-enabled local processes. The data mover receiving the NFS request decodes the request to verify the RPC portion of the request and check's the client's authorization for the desired access (Col. 14, lines 1-5). If the request is not authenticated and authorized then execution of the request is rejected (Col. 14, lines 5-7). Otherwise, the request is granted (Col. 14, lines 7-8), which meets the limitation of wherein said network file system examines said requests, and either grants or denies each of said requests depending on whether the request is justifiable from a security perspective by using information that includes, but is not limited to: the nature of the originating streaming-enabled process, the history of previous access by the streaming-enabled process, and/or the

Art Unit: 2132

section of the targeted streaming application program file being requested. If the request is granted then the data mover processing the request discovers the path to the desired file and sends a request to the remote file system corresponding to the file for access (Col. 14, lines 9-35). Each read/write file system is assigned a primary data mover with respect to the file system (Col. 13, lines 31-33). This data mover has the exclusive right to directly access data in each file in the read/write file system, and manages the read and write locks on the files in the file system (Col. 13, lines 33-38). When a data mover receives a request for access from a client terminal, the data mover checks the type of request and the database of the file system for which it is serving to determine whether they can process the request or whether the request must be processed by a different data mover (Col. 13, lines 38-64), which meets the limitation of wherein said file system registers dispatch routines with the client operating system that handle common file operations such as open, read write, and close, wherein a dispatch routine examines a file request and decides whether to grant or deny said file request, wherein if said file request is granted, then said dispatch routine allows the requested operation to proceed.

Referring to claim 31, Vahalia discloses a data storage system wherein a network file server containing an array of data movers, and a disk storage subsystem (Figure 1), provides high-end file server applications such as the Network File System (NFS) protocol standard (Col. 5, lines 40-43). The system processes and receives NFS data requests from a client computer (Col. 13, lines 66-67), which meets the limitation of providing a network file system on a client, using a filtering mechanism that is associated with said second computer for filtering requests for access to said streaming application program files. The data is provided over the system in a streaming fashion (Col. 7, lines 13-29), which meets the limitation of using a first computer to

serve streaming application program files to a second computer for execution. The client terminal provides NFS data requests over the network that are processed by a data mover of the network file server (Col. 13, lines 66-67), which makes the limitation of streaming-enabled local processes on the client and inherent feature of Vahalia because the use of the NFS protocol requires streaming-enabled local processes. The data mover receiving the NFS request decodes the request to verify the RPC portion of the request and check's the client's authorization for the desired access (Col. 14, lines 1-5). If the request is not authenticated and authorized then execution of the request is rejected (Col. 14, lines 5-7). Otherwise, the request is granted (Col. 14, lines 7-8), which meets the limitation of wherein said network file system examines said requests, and either grants or denies each of said requests depending on whether the request is justifiable from a security perspective by using information that includes, but is not limited to: the nature of the originating streaming-enabled process, the history of previous access by the streaming-enabled process, and/or the section of the targeted streaming application program file being requested. Clients have a security level associated with them in order to control access to files containing sensitive material (Col. 17, lines 7-10), which meets the limitation of determining whether the section of said streaming application program files that is being requested is a critical section.

Referring to claim 32, Vahalia discloses a data storage system wherein a network file server containing an array of data movers, and a disk storage subsystem (Figure 1), provides high-end file server applications such as the Network File System (NFS) protocol standard (Col. 5, lines 40-43). The system processes and receives NFS data requests from a client computer (Col. 13, lines 66-67). The data is provided over the system in a streaming fashion (Col. 7, lines



Art Unit: 2132

13-29), which meets the limitation of streaming application program files. The client terminal provides NFS data requests over the network that are processed by a data mover of the network file server (Col. 13, lines 66-67). The data mover receiving the NFS request decodes the request to verify the RPC portion of the request and check's the client's authorization for the desired access (Col. 14, lines 1-5). If the request is not authenticated and authorized then execution of the request is rejected (Col. 14, lines 5-7). Otherwise, the request is granted (Col. 14, lines 7-8), which meets the limitation of determining whether an originating process that is making said requests for access is a trusted process. If the request is granted then the data mover processing the request discovers the path to the desired file and sends a request to the remote file system corresponding to the file for access (Col. 14, lines 9-35), which meets the limitation of providing information relating to one or more remote locations where streaming application program files are stored. Clients have a security level associated with them in order to control access to files containing sensitive material (Col. 17, lines 7-10), which meets the limitation of determining whether the section of said streaming application program files that is being requested is a critical section. Applicant's specification (page 4) defines a pattern of piracy as an attempt to copy as opposed to code execution. Vahalia discloses that each file contains read and write locks that can be enabled depending on how the content owners want the content to be accessed. The locks can be enabled so that the content can only be read or code executed, and if the client requests to write the file, then the request is denied (Col. 17, line 58 – Col. 18, line 8), which meets the limitation of determining whether an originating process making the request for access exhibits a pre-determined pattern of piracy.

Referring to claim 33, Vahalia discloses a data storage system wherein a network file server containing an array of data movers, and a disk storage subsystem (Figure 1), provides high-end file server applications such as the Network File System (NFS) protocol standard (Col. 5, lines 40-43). The system processes and receives NFS data requests from a client computer (Col. 13, lines 66-67), which meets the limitation of using dispatch routines for examining a request for access to said streaming application program files. The data is provided over the system in a streaming fashion (Col. 7, lines 13-29), which meets the limitation of streaming application program files. The client terminal provides NFS data requests over the network that are processed by a data mover of the network file server (Col. 13, lines 66-67). The data mover receiving the NFS request decodes the request to verify the RPC portion of the request and check's the client's authorization for the desired access (Col. 14, lines 1-5). If the request is not authenticated and authorized then execution of the request is rejected (Col. 14, lines 5-7). Otherwise, the request is granted (Col. 14, lines 7-8), which meets the limitation of after examining said request and if it is determined that an originating process that is making said request for access is a trusted process, then forwarding said request to a corresponding remote server that is responsible for serving said streaming application program files. If the request is granted then the data mover processing the request discovers the path to the desired file and sends a request to the remote file system corresponding to the file for access (Col. 14, lines 9-35), which meets the limitation of providing information relating to one or more remote locations where streaming application program files are stored. Clients have a security level associated with them in order to control access to files containing sensitive material (Col. 17, lines 7-10), which meets the limitation of determining whether the section of said streaming application

Art Unit: 2132

program files that is being requested is a critical section. Applicant's specification (page 4) defines a pattern of piracy as an attempt to copy as opposed to code execution. Vahalia discloses that each file contains read and write locks that can be enabled depending on how the content owners want the content to be accessed. The locks can be enabled so that the content can only be read or code executed, and if the client requests to write the file, then the request is denied (Col. 17, line 58 – Col. 18, line 8), which meets the limitation of determining whether an originating process making the request for access exhibits a pre-determined pattern of piracy.

Referring to claim 34, Vahalia discloses a data storage system wherein a network file server containing an array of data movers, and a disk storage subsystem (Figure 1), provides high-end file server applications such as the Network File System (NFS) protocol standard (Col. 5, lines 40-43). The system processes and receives NFS data requests from a client computer (Col. 13, lines 66-67), which meets the limitation of using a filtering mechanism on a client computer for filtering requests for access to streaming application program files. The data is provided over the system in a streaming fashion (Col. 7, lines 13-29), which meets the limitation of streaming application program files. The client terminal provides NFS data requests over the network that are processed by a data mover of the network file server (Col. 13, lines 66-67). The data mover receiving the NFS request decodes the request to verify the RPC portion of the request and check's the client's authorization for the desired access (Col. 14, lines 1-5). If the request is not authenticated and authorized then execution of the request is rejected (Col. 14, lines 5-7). Otherwise, the request is granted (Col. 14, lines 7-8), which meets the limitation of wherein said filtering mechanism determines whether to grant requests for access to said streaming application program files by determining one or more criteria from a set of criteria

comprising: the nature of the originating streaming-enabled process, the history of previous access by the streaming-enabled process, and the section of the targeted streaming application program file being requested. If the request is granted then the data mover processing the request discovers the path to the desired file and sends a request to the remote file system corresponding to the file for access (Col. 14, lines 9-35), which meets the limitation of using a revealing mechanism to reveal to said client computer one or more remote locations on which said requested streaming application program files are stored. Clients have a security level associated with them in order to control access to files containing sensitive material (Col. 17, lines 7-10), which meets the limitation of determining whether the section of said streaming application program files that is being requested is a critical section.

Referring to claim 35, Vahalia discloses a data storage system wherein a network file server containing an array of data movers, and a disk storage subsystem (Figure 1), provides high-end file server applications such as the Network File System (NFS) protocol standard (Col. 5, lines 40-43). The system processes and receives NFS data requests from a client computer (Col. 13, lines 66-67), which meets the limitation of processing device for processing a request for access to streaming application program files stored on at least one server system that is remote from said processing device. The data is provided over the system in a streaming fashion (Col. 7, lines 13-29), which meets the limitation of streaming application program files. The client terminal provides NFS data requests over the network that are processed by a data mover of the network file server (Col. 13, lines 66-67). The data mover receiving the NFS request decodes the request to verify the RPC portion of the request and check's the client's authorization for the desired access (Col. 14, lines 1-5). If the request is not authenticated and

Art Unit: 2132

authorized then execution of the request is rejected (Col. 14, lines 5-7). Otherwise, the request is granted (Col. 14, lines 7-8), which meets the limitation of wherein said processing device comprises a component that determines whether to grant requests for access to said streaming application program files based on: whether an originating process that is making said requests for access is a trusted process. If the request is granted then the data mover processing the request discovers the path to the desired file and sends a request to the remote file system corresponding to the file for access (Col. 14, lines 9-35), which meets the limitation of using a revealing mechanism to reveal to said client computer one or more remote locations on which said requested streaming application program files are stored. Clients have a security level associated with them in order to control access to files containing sensitive material (Col. 17, lines 7-10), which meets the limitation of determining whether the section of said streaming application program files that is being requested is a critical section. Applicant's specification (page 4) defines a pattern of piracy as an attempt to copy as opposed to code execution. Vahalia discloses that each file contains read and write locks that can be enabled depending on how the content owners want the content to be accessed. The locks can be enabled so that the content can only be read or code executed, and if the client requests to write the file, then the request is denied (Col. 17, line 58 – Col. 18, line 8), which meets the limitation of determining whether an originating process making the request for access exhibits a pre-determined pattern of piracy.

Referring to claim 36, Vahalia discloses a data storage system wherein a network file server containing an array of data movers, and a disk storage subsystem (Figure 1), provides high-end file server applications such as the Network File System (NFS) protocol standard (Col. 5, lines 40-43). The system processes and receives NFS data requests from a client computer

Art Unit: 2132

(Col. 13, lines 66-67), which meets the limitation of processing means for processing requests for access to streaming application program files stored remotely from said processing means. The data is provided over the system in a streaming fashion (Col. 7, lines 13-29), which meets the limitation of streaming application program files. The client terminal provides NFS data requests over the network that are processed by a data mover of the network file server (Col. 13, lines 66-67). The data mover receiving the NFS request decodes the request to verify the RPC portion of the request and check's the client's authorization for the desired access (Col. 14, lines 1-5). If the request is not authenticated and authorized then execution of the request is rejected (Col. 14, lines 5-7). Otherwise, the request is granted (Col. 14, lines 7-8), which meets the limitation of wherein said processing means includes a determination means for determining whether to grant requests for access to said streaming application program files based on: whether an originating process that is making said requests for access is a trusted process. If the request is granted then the data mover processing the request discovers the path to the desired file and sends a request to the remote file system corresponding to the file for access (Col. 14, lines 9-35), which meets the limitation of a redirection means for revealing one or more remote locations in which said requested streaming application program files are stored. Clients have a security level associated with them in order to control access to files containing sensitive material (Col. 17, lines 7-10), which meets the limitation of determining whether the section of said streaming application program files that is being requested is a critical section. Applicant's specification (page 4) defines a pattern of piracy as an attempt to copy as opposed to code execution. Vahalia discloses that each file contains read and write locks that can be enabled depending on how the content owners want the content to be accessed. The locks can be enabled

so that the content can only be read or code executed, and if the client requests to write the file, then the request is denied (Col. 17, line 58 – Col. 18, line 8), which meets the limitation of determining whether an originating process making the request for access exhibits a pre-determined pattern of piracy.

Referring to claim 37, Vahalia discloses a data storage system wherein a network file server containing an array of data movers, and a disk storage subsystem (Figure 1), provides high-end file server applications such as the Network File System (NFS) protocol standard (Col. 5, lines 40-43). The system processes and receives NFS data requests from a client computer (Col. 13, lines 66-67), which meets the limitation of using a filtering means for filtering requests for access to streaming application program files stored remotely from said filtering means. The data is provided over the system in a streaming fashion (Col. 7, lines 13-29), which meets the limitation of streaming application program files. The client terminal provides NFS data requests over the network that are processed by a data mover of the network file server (Col. 13, lines 66-67). The data mover receiving the NFS request decodes the request to verify the RPC portion of the request and check's the client's authorization for the desired access (Col. 14, lines 1-5). If the request is not authenticated and authorized then execution of the request is rejected (Col. 14, lines 5-7). Otherwise, the request is granted (Col. 14, lines 7-8), which meets the limitation of wherein said filtering means includes an evaluation means for evaluating: the nature of the originating streaming-enabled process, the history of previous access by the streaming-enabled process, and the section of the targeted streaming application program file being requested. If the request is granted then the data mover processing the request discovers the path to the desired file and sends a request to the remote file system corresponding to the file for access (Col. 14,

lines 9-35), which meets the limitation of a redirection means for revealing one or more locations in which said requested streaming application program files are stored. Clients have a security level associated with them in order to control access to files containing sensitive material (Col. 17, lines 7-10), which meets the limitation of determining whether the section of said streaming application program files that is being requested is a critical section.

Referring to claim 38, Vahalia discloses a data storage system wherein a network file server containing an array of data movers, and a disk storage subsystem (Figure 1), provides high-end file server applications such as the Network File System (NFS) protocol standard (Col. 5, lines 40-43). The system processes and receives NFS data requests from a client computer (Col. 13, lines 66-67). The data is provided over the system in a streaming fashion (Col. 7, lines 13-29), which meets the limitation of streaming application program files. The client terminal provides NFS data requests over the network that are processed by a data mover of the network file server (Col. 13, lines 66-67). The data mover receiving the NFS request decodes the request to verify the RPC portion of the request and check's the client's authorization for the desired access (Col. 14, lines 1-5). If the request is not authenticated and authorized then execution of the request is rejected (Col. 14, lines 5-7). Otherwise, the request is granted (Col. 14, lines 7-8), which meets the limitation of determining whether an originating process that is making said requests for access is a trusted process. If the request is granted then the data mover processing the request discovers the path to the desired file and sends a request to the remote file system corresponding to the file for access (Col. 14, lines 9-35), which meets the limitation of providing information relating to one or more remote locations where streaming application program files are stored. Clients have a security level associated with them in order to control access to files



containing sensitive material (Col. 17, lines 7-10), which meets the limitation of determining whether the section of said streaming application program files that is being requested is a critical section. Applicant's specification (page 4) defines a pattern of piracy as an attempt to copy as opposed to code execution. Vahalia discloses that each file contains read and write locks that can be enabled depending on how the content owners want the content to be accessed. The locks can be enabled so that the content can only be read or code executed, and if the client requests to write the file, then the request is denied (Col. 17, line 58 – Col. 18, line 8), which meets the limitation of determining whether an originating process making the request for access exhibits a pre-determined pattern of piracy.

Referring to claim 39, Vahalia discloses a data storage system wherein a network file server containing an array of data movers, and a disk storage subsystem (Figure 1), provides high-end file server applications such as the Network File System (NFS) protocol standard (Col. 5, lines 40-43). The system processes and receives NFS data requests from a client computer (Col. 13, lines 66-67), which meets the limitation of processing device for processing a request for access to streaming application program files stored on at least one server system that is remote from said processing device. The data is provided over the system in a streaming fashion (Col. 7, lines 13-29), which meets the limitation of streaming application program files. The client terminal provides NFS data requests over the network that are processed by a data mover of the network file server (Col. 13, lines 66-67). The data mover receiving the NFS request decodes the request to verify the RPC portion of the request and check's the client's authorization for the desired access (Col. 14, lines 1-5). If the request is not authenticated and authorized then execution of the request is rejected (Col. 14, lines 5-7). Otherwise, the request is

Art Unit: 2132

granted (Col. 14, lines 7-8), which meets the limitation of after examining said request and if it is determined that an originating process that is making said request for access is a trusted process, then forwarding said request to a corresponding remote server that is responsible for serving said streaming application program files. If the request is granted then the data mover processing the request discovers the path to the desired file and sends a request to the remote file system corresponding to the file for access (Col. 14, lines 9-35), which meets the limitation of providing information relating to one or more remote locations where streaming application program files are stored. Clients have a security level associated with them in order to control access to files containing sensitive material (Col. 17, lines 7-10), which meets the limitation of determining whether the section of said streaming application program files that is being requested is a critical section. Applicant's specification (page 4) defines a pattern of piracy as an attempt to copy as opposed to code execution. Vahalia discloses that each file contains read and write locks that can be enabled depending on how the content owners want the content to be accessed. The locks can be enabled so that the content can only be read or code executed, and if the client requests to write the file, then the request is denied (Col. 17, line 58 – Col. 18, line 8), which meets the limitation of determining whether an originating process making the request for access exhibits a pre-determined pattern of piracy.

Referring to claim 40, Vahalia discloses a data storage system wherein a network file server containing an array of data movers, and a disk storage subsystem (Figure 1), provides high-end file server applications such as the Network File System (NFS) protocol standard (Col. 5, lines 40-43). The system processes and receives NFS data requests from a client computer (Col. 13, lines 66-67). The data is provided over the system in a streaming fashion (Col. 7, lines

Art Unit: 2132

13-29), which meets the limitation of streaming application program files. The client terminal provides NFS data requests over the network that are processed by a data mover of the network file server (Col. 13, lines 66-67). The data mover receiving the NFS request decodes the request to verify the RPC portion of the request and check's the client's authorization for the desired access (Col. 14, lines 1-5). If the request is not authenticated and authorized then execution of the request is rejected (Col. 14, lines 5-7). Otherwise, the request is granted (Col. 14, lines 7-8), which meets the limitation of determining whether an originating process that is making said requests for access is a trusted process. If the request is granted then the data mover processing the request discovers the path to the desired file and sends a request to the remote file system corresponding to the file for access (Col. 14, lines 9-35), which meets the limitation of providing information relating to one or more remote locations where streaming application program files are stored. Clients have a security level associated with them in order to control access to files containing sensitive material (Col. 17, lines 7-10), which meets the limitation of determining whether the section of said streaming application program files that is being requested is a critical section. Applicant's specification (page 4) defines a pattern of piracy as an attempt to copy as opposed to code execution. Vahalia discloses that each file contains read and write locks that can be enabled depending on how the content owners want the content to be accessed. The locks can be enabled so that the content can only be read or code executed, and if the client requests to write the file, then the request is denied (Col. 17, line 58 – Col. 18, line 8), which meets the limitation of determining whether an originating process making the request for access exhibits a pre-determined pattern of piracy.

Referring to claim 41, Vahalia discloses a data storage system wherein a network file server containing an array of data movers, and a disk storage subsystem (Figure 1), provides high-end file server applications such as the Network File System (NFS) protocol standard (Col. 5, lines 40-43). The system processes and receives NFS data requests from a client computer (Col. 13, lines 66-67), which meets the limitation of a means for examining requests for access to said streaming application program files. The data is provided over the system in a streaming fashion (Col. 7, lines 13-29), which meets the limitation of streaming application program files. The client terminal provides NFS data requests over the network that are processed by a data mover of the network file server (Col. 13, lines 66-67). The data mover receiving the NFS request decodes the request to verify the RPC portion of the request and check's the client's authorization for the desired access (Col. 14, lines 1-5). If the request is not authenticated and authorized then execution of the request is rejected (Col. 14, lines 5-7). Otherwise, the request is granted (Col. 14, lines 7-8), which meets the limitation of a means for determining whether said requests can be granted based on whether an originating process that is making said request for access is a trusted process, a means for forwarding said request to a corresponding remote server that is responsible for serving said streaming application program files if said requests are granted. If the request is granted then the data mover processing the request discovers the path to the desired file and sends a request to the remote file system corresponding to the file for access (Col. 14, lines 9-35), which meets the limitation of a means for providing information to a local computing system of streaming application program files that are stored on one or more remote locations. Clients have a security level associated with them in order to control access to files containing sensitive material (Col. 17, lines 7-10), which meets the limitation of determining

whether the section of said streaming application program files that is being requested is a critical section. Applicant's specification (page 4) defines a pattern of piracy as an attempt to copy as opposed to code execution. Vahalia discloses that each file contains read and write locks that can be enabled depending on how the content owners want the content to be accessed. The locks can be enabled so that the content can only be read or code executed, and if the client requests to write the file, then the request is denied (Col. 17, line 58 – Col. 18, line 8), which meets the limitation of determining whether an originating process making the request for access exhibits a pre-determined pattern of piracy.

Referring to claim 42, Vahalia discloses a data storage system wherein a network file server containing an array of data movers, and a disk storage subsystem (Figure 1), provides high-end file server applications such as the Network File System (NFS) protocol standard (Col. 5, lines 40-43). The system processes and receives NFS data requests from a client computer (Col. 13, lines 66-67), which meets the limitation of receiving a request from a computer process for access to said streaming application program files. The data is provided over the system in a streaming fashion (Col. 7, lines 13-29), which meets the limitation of streaming application program files. The client terminal provides NFS data requests over the network that are processed by a data mover of the network file server (Col. 13, lines 66-67). The data mover receiving the NFS request decodes the request to verify the RPC portion of the request and check's the client's authorization for the desired access (Col. 14, lines 1-5). If the request is not authenticated and authorized then execution of the request is rejected (Col. 14, lines 5-7). Otherwise, the request is granted (Col. 14, lines 7-8), which meets the limitation of determining if said computer process that is making said request for access is a trusted process. If the request

is granted then the data mover processing the request discovers the path to the desired file and sends a request to the remote file system corresponding to the file for access (Col. 14, lines 9-35), which meets the limitation of providing information relating to one or more remote locations where streaming application program files are stored, if said computer process is a trusted process, then forwarding said request to a corresponding remote server that is responsible for serving said streaming application program files.

Referring to claim 43, Vahalia discloses a data storage system wherein a network file server containing an array of data movers, and a disk storage subsystem (Figure 1), provides high-end file server applications such as the Network File System (NFS) protocol standard (Col. 5, lines 40-43). The system processes and receives NFS data requests from a client computer (Col. 13, lines 66-67), which meets the limitation of receiving a request from a computer process for access to said streaming application program files. The data is provided over the system in a streaming fashion (Col. 7, lines 13-29), which meets the limitation of streaming application program files. The client terminal provides NFS data requests over the network that are processed by a data mover of the network file server (Col. 13, lines 66-67). The data mover receiving the NFS request decodes the request to verify the RPC portion of the request and check's the client's authorization for the desired access (Col. 14, lines 1-5). If the request is not authenticated and authorized then execution of the request is rejected (Col. 14, lines 5-7). Otherwise, the request is granted (Col. 14, lines 7-8). Applicant's specification (page 4) defines a pattern of piracy as an attempt to copy as opposed to code execution. Vahalia discloses that each file contains read and write locks that can be enabled depending on how the content owners want the content to be accessed. The locks can be enabled so that the content can only be read or code

Art Unit: 2132

executed, and if the client requests to write the file, then the request is denied (Col. 17, line 58 – Col. 18, line 8), which meets the limitation of determining whether an originating process making the request for access exhibits a pre-determined pattern of piracy. If the request is granted then the data mover processing the request discovers the path to the desired file and sends a request to the remote file system corresponding to the file for access (Col. 14, lines 9-35), which meets the limitation of providing information relating to one or more remote locations where streaming application program files are stored, if said computer process lacks a pre-determined pattern of piracy, then forwarding said request to a corresponding remote server that is responsible for serving said streaming application program files.

Referring to claim 44, Vahalia discloses a data storage system wherein a network file server containing an array of data movers, and a disk storage subsystem (Figure 1), provides high-end file server applications such as the Network File System (NFS) protocol standard (Col. 5, lines 40-43). The system processes and receives NFS data requests from a client computer (Col. 13, lines 66-67), which meets the limitation of receiving a request from a computer process for access to said streaming application program files. The data is provided over the system in a streaming fashion (Col. 7, lines 13-29), which meets the limitation of streaming application program files. The client terminal provides NFS data requests over the network that are processed by a data mover of the network file server (Col. 13, lines 66-67). The data mover receiving the NFS request decodes the request to verify the RPC portion of the request and check's the client's authorization for the desired access (Col. 14, lines 1-5). If the request is not authenticated and authorized then execution of the request is rejected (Col. 14, lines 5-7). Otherwise, the request is granted (Col. 14, lines 7-8). Clients have a security level associated

Art Unit: 2132

with them in order to control access to files containing sensitive material (Col. 17, lines 7-10), which meets the limitation of determining if said section that is being requested is a non-critical section. If the request is granted then the data mover processing the request discovers the path to the desired file and sends a request to the remote file system corresponding to the file for access (Col. 14, lines 9-35), which meets the limitation of providing information relating to one or more remote locations where streaming application program files are stored, if said section is a non-critical section, then forwarding said request to a corresponding remote server that is responsible for serving said streaming application program files.

6. Claims 31-42 are rejected under 35 U.S.C. 102(e) as being anticipated by Safadi, U.S. Patent No. 6,810,525. Referring to claim 31, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of using a first computer to serve said application program files to a second computer for execution, using a filtering mechanism that is associated with said second computer for filtering requests for access to said application program files, wherein said filtering mechanism determines whether to grant requests for access to said application program files by determining one or more criteria from a set of criteria comprising: a nature of an originating process that is making said requests for access, a history of previous requests for access made by said originating process, and a nature of a section of said application program files that is being requested. The multimedia servers can be streaming (Abstract), which meets the limitation of streaming application program files.



Referring to claim 32, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of providing information relating to one or more remote locations where said application program files are stored, determining whether an originating process that is making said requests for access is a trusted process, whether a history of previous requests for access made by said originating process exhibits a pre-determined pattern of piracy, and whether a section of said application program files that is being requested is a critical section that requires protection from piracy. The multimedia servers can be streaming (Abstract), which meets the limitation of streaming application program files.

Referring to claims 33, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17). The client application of Safadi would meet the limitation of the dispatch routine that examines the file requests and decides whether to grant or deny said file request (Col. 2, lines 1-10, Col. 3, lines 11-17). which meets the limitation of providing information relating to one or more remote locations where said application program files are stored, using dispatch routines for examining a request for access to said application program files, after examining said request and if it is determined that an originating process that is making said request for access is a trusted process, or that a history of previous requests for access made by said originating process lacks a pre-determined pattern of piracy, and that a

Art Unit: 2132

section of said application program files that is being requested is a non-critical section, then forwarding said request to a corresponding remote server that is responsible for serving said application program files. The multimedia servers can be streaming (Abstract), which meets the limitation of streaming application program files.

Referring to claim 34, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of using a filtering mechanism on a client computer for filtering requests for access to said application program files, wherein said filtering mechanism determines whether to grant requests for access to said application program files by determining one or more criteria from a set of criteria comprising: a nature of an originating process that is making said requests for access, a history of previous requests for access made by said originating process, and a nature of a section of said application program files that is being requested. The client application then sends the entitlement token to a proxy server in order to determine the status of the subscriber's request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of using a revealing mechanism to reveal to said client computer one or more remote locations on which said requested application program files are stored. The multimedia servers can be streaming (Abstract), which meets the limitation of streaming application program files.

Referring to claim 35, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be

Art Unit: 2132

authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of a processing device for processing a request for access to said application program files stored on at least one server system that is remote from said processing device, wherein said processing device comprises a component that determines whether to grant requests for access to said application program files based on: whether an originating process that is making said requests for access is a trusted process, whether a history of previous requests for access made by said originating process exhibits a pre-determined pattern of piracy, and whether a section of said application program files that is being requested is a critical section that requires protection from piracy. The client application then sends the entitlement token to a proxy server in order to determine the status of the subscriber's request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of a redirecting component that is associated with said processing device for informing said processing device of one or more locations in which said application program files are stored. The multimedia servers can be streaming (Abstract), which meets the limitation of streaming application program files.

Referring to claim 36, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of processing means for processing a request for access to said application program files stored remotely from said processing means, wherein said processing means includes a determination whether to grant

requests for access to said application program files based on: whether an originating process that is making said requests for access is a trusted process, whether a history of previous requests for access made by said originating process exhibits a pre-determined pattern of piracy, and whether a section of said application program files that is being requested is a critical section that requires protection from piracy. The client application then sends the entitlement token to a proxy server in order to determine the status of the subscriber's request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of a redirection means for revealing one or more locations in which said application program files are stored. The multimedia servers can be streaming (Abstract), which meets the limitation of streaming application program files.

Referring to claim 37, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of a filtering means for filtering requests for access to said application program files stored remotely from said filtering means, wherein said filtering means includes an evaluation means for evaluating: an originating process that is making said requests for access, a history of previous requests for access made by said originating process, and a section of said application program files that is being requested. The client application then sends the entitlement token to a proxy server in order to determine the status of the subscriber's request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of a redirection means for revealing one or more locations in which said requested

application program files are stored. The multimedia servers can be streaming (Abstract), which meets the limitation of streaming application program files.

Referring to claim 38, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of determining whether an originating process that is making said requests for access is a trusted process, whether a history of previous requests for access made by said originating process exhibits a pre-determined pattern of piracy, and whether a section of said application program files that is being requested is a critical section that requires protection from piracy. The client application then sends the entitlement token to a proxy server in order to determine the status of the subscriber's request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of providing information relating to one or more remote locations where said application program files are stored. The multimedia servers can be streaming (Abstract), which meets the limitation of streaming application program files.

Referring to claim 39, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of using dispatch routines for examining a request for access to said application program files, after examining said request and if it is determined that an originating process that is making said request for

access is a trusted process, and that a history of previous requests for access made by said originating process lacks a pre-determined pattern of piracy, and that a section of said application program files that is being requested is a non-critical section, then forwarding said request to a corresponding remote server that is responsible for serving said application program files. The client application then sends the entitlement token to a proxy server in order to determine the status of the subscriber's request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of providing information relating to one or more remote locations where said application program files are stored. The multimedia servers can be streaming (Abstract), which meets the limitation of streaming application program files.

Referring to claim 40, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of determining whether an originating process that is making said request for access is a trusted process, whether a history of previous requests for access made by said originating process exhibits a pre-determined pattern of piracy, and whether a section of said application program files that is being requested is a critical section that requires protection from piracy. The client application then sends the entitlement token to a proxy server in order to determine the status of the subscriber's request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of providing information relating to one or more remote locations where said application program files are stored. The

multimedia servers can be streaming (Abstract), which meets the limitation of streaming application program files.

Referring to claim 41, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1, line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of a means for examining requests for access to said application program files, a means for determining whether said requests can be granted based on whether an originating process that is making said requests for access is a trusted process, whether a history of previous requests for access made by said originating process exhibits a predetermined pattern of piracy, and whether a section of said application program files that is being requested is a critical section that requires protection from piracy, if said requests are granted then forwarding said requests to a corresponding server that is responsible for serving said application program files. The client application then sends the entitlement token to a proxy server in order to determine the status of the subscriber's request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of a means for providing location information to a local computing system of said application program files that are stored on one or more remote locations. The multimedia servers can be streaming (Abstract), which meets the limitation of streaming application program files.

Referring to claim 42, Safadi discloses a system for multimedia services wherein a user requests use of a specific data services by creating a secure entitlement token that can be authenticated by a client application at the subscriber terminal based on a credit amount (Col. 1,

Art Unit: 2132

line 62 – Col. 2, line 10, Col. 3, lines 11-17), which meets the limitation of receiving a request from a computer process for access to said application program files, determining if said computer process that is making said request for access is a trusted process, if said computer process is a trusted process, then forwarding said request to a corresponding remote server that is responsible for serving said application program files. The client application then sends the entitlement token to a proxy server in order to determine the status of the subscriber's request, and if the request was verified then enabling the selected service/application for use by the subscriber from ISP (Col. 2, line 11-24), which meets the limitation of providing information relating to one or more remote locations where said application program files are stored. The multimedia servers can be streaming (Abstract), which meets the limitation of streaming application program files.

### ***Conclusion***

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

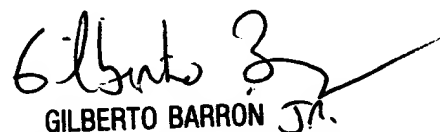


Art Unit: 2132

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Benjamin E. Lanier



GILBERTO BARRON JR.  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100